IN THE CLAIMS

Claims 1-39 (cancelled)

40. (previously presented) A device for use in an information processing system that distributes encrypted message data, the device comprising:

a receiver for receiving the encrypted message data and an enabling key block (EKB), the EKB including encrypted keys and a tag, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

a memory for storing a key set, the key set including at least one key corresponding to a node or leaf of the hierarchical tree structure; and

an encryption processor operable to (a) decrypt the encrypted keys of the received EKB using the stored key set and the position discrimination data of the received EKB to recover the at least one renewed key and (b) decrypt the received encrypted message using the at least one recovered renewed key.

41. (Previously presented) The device of claim 40, wherein the at least one renewed key is associated with a predetermined node of the hierarchical tree structure and is encrypted using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node.

42. (previously presented) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a

terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

43. (previously presented) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB further indicates whether an encrypted key corresponding to a predetermined node is included in the EKB and, if included, the position discrimination data indicates whether that encrypted key is at a left or right node position of the simplified tree structure which is subordinate to the predetermined node.

44. (previously presented) The device of claim 43, wherein the simplified tree structure comprises a sub-root that is a top node of an entity.

45. (previously presented) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a top node and a terminal node of a simplified tree structure, the simplified tree being constructed from the hierarchical tree structure by selecting only paths between the top node and the terminal node of the hierarchical tree structure, and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

46. (previously presented) The device of claim 45, wherein the simplified tree structure is a tree having not less than three branches connecting the top node with the terminal node.

47. (previously presented) The device of claim 40, wherein the encryption processor is operable to sequentially (a) extract the encrypted keys from the received EKB using the position discrimination data from the tag, (b) decrypt the extracted encrypted keys to obtain the renewed key, and (c) decrypt the received encrypted message using the renewed key.

48. (previously presented) The device of claim 40, wherein the encrypted message data represents a content key that can be used as a decryption key for decrypting encrypted content.

49. (previously presented) The device of claim 40, wherein the encrypted message data represents an authentication key used in an authentication process.

50. (previously presented) The device of claim 40, wherein the encrypted message data represents a key for generating an integrity check value (ICV) of content.

51. (previously presented) The device of claim 40, wherein the encrypted message data represents program code.

Claims 52-67 (canceled)

68. (previously presented) An information processing system, comprising:

means for receiving encrypted message data and an enabling key block (EKB), the EKB including encrypted keys and a tag, the encrypted keys including at least one renewed key and

the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

means for storing a key set, the key set including at least one key corresponding to a node or leaf of the hierarchical tree structure; and

means for decrypting the encrypted keys of the received EKB using the stored key set and the position discrimination data of the received EKB to recover the at least one renewed key and for decrypting the received encrypted message using the at least one recovered renewed key.

69. (previously presented) The information processing system according to claim 68, wherein the at least one renewed key is associated with a predetermined node of the hierarchical tree structure and is encrypted using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node.

70. (previously presented) The information processing system according to claim 68, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

71. (previously presented) The information processing system according to claim 68, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being

constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB further indicates whether an encrypted key corresponding to a predetermined node is included in the EKB and, if included, the position discrimination data indicates whether that encrypted key is at a left or right node position of the simplified tree structure which is subordinate to the predetermined node.

72. (previously presented) The information processing system according to claim 68, wherein the decrypting means sequentially (a) extracts the encrypted keys from the received EKB using the position discriminates data from the tag, (b) decrypts the extracted encrypted keys to obtain the renewed key, and (c) decrypts the received encrypted message using the renewed key.

73. (previously presented) An information processing method for use in decrypting encrypted message data, the method comprising:

receiving an enabling key block (EKB) including encrypted keys and a tag, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

extracting the encrypted keys from the received EKB in accordance with the positional discrimination data from the tag; and

decrypting the extracted encrypted keys to obtain the at least one renewed key.

74. (previously presented) The information processing method according to claim 73, wherein the decrypting step includes using a stored key set to decrypt the extracted encrypted keys, the stored key set including at least one key corresponding to a node or leaf of the hierarchical tree structure.

75. (previously presented) The information processing method according to claim 73, further comprising decrypting encrypted message data using the at least one obtained renewed key.

76. (previously presented) The information processing method according to claim 75, wherein the encrypted message data represents a content key that can be used as a decryption key for decrypting encrypted content.

77. (previously presented) The information processing method according to claim 75, wherein the encrypted message data represents an authentication key used in an authentication process.

78. (previously presented) The information processing method according to claim 75, wherein the encrypted message data represents a key for generating an integrity check value (ICV) of content.

79. (previously presented) The information processing method according to claim 75, wherein the encrypted message data represents program code.